UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

KEVIN WALLES and JOSE VARGAS, on behalf of themselves and all others similarly situated, Plaintiffs, v. AUTOZONE, INC. and PROGRESS SOFTWARE CORPORATION, Defendants.	Case No.: _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs, Kevin Walles and Jose Vargas ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendant AutoZone, Inc. ("AutoZone") and Defendant Progress Software Corporation ("PSC") (collectively, "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents, as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated AutoZone employees' sensitive information, including their full names and Social Security numbers ("personally identifiable information" or "PII").

2. Defendant AutoZone is "leading retailer and a leading distributor of automotive replacement parts and accessories in the U.S."[1]

[1] https://about.autozone.com/

3. Defendant PSC advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[2]

4. Upon information and belief, former and current AutoZone employees are required to entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to obtain employment from AutoZone. Defendants retain this information for at least many years and even after the relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. On an undisclosed date, AutoZone learned that Pension Benefit Information, LLC's network, to whom PSC provided software services, and for which AutoZone relied on for the sending and receiving of sensitive information, had been penetrated by a cyberattack.[3] In response, AutoZone "commenced an investigation, retained outside experts, and took measures to assess and remediate incident."[4] As a result of the investigation, AutoZone concluded–on or about August 15, 2023–that "the exploitation of the vulnerability in the MOVEit application had resulted in the exfiltration of certain data."[5]

7. According to the Notice of Data Incident letter sent by AutoZone, on behalf of Defendants, to Plaintiffs and other victims of the Data Breach (the "Notice Letter"), the

[2] https://www.progress.com/company
[3] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/4b650bee-f556-4b08-8659-f0e1207aa969.shtml
[4] *Id.*
[5] *Id.*

compromised PII included individuals' full names and Social Security numbers.[6]

8. Defendants failed to adequately protect Plaintiffs' and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect employees' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

10. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by their IT vendors to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in

[6] *Id.*

ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Vargas experiencing fraud in the form of an identity thief using his PII to submit a loan application to Upside, in or about November 2023; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

12. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect AutoZone's employees' PII from a foreseeable and preventable cyber-attack.

13. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

14. Plaintiff, Kevin Walles, is, and at all times mentioned herein was, an individual

and citizen of Aurora, Missouri.

15. Plaintiff, Jose Vargas, is, and at all times mentioned herein was, an individual and citizen of Santa Ana, California.

16. Defendant, AutoZone, Inc., is a corporation incorporated under the state laws of Nevada with its principal place of business located at 123 South Front Street, Memphis, Tennessee 38103.

17. Defendant, Progress Software Corporation, is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Massachusetts and have different citizenship from Defendants, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

19. This Court has jurisdiction over Defendants because Defendants operate in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant PSC's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendants' Businesses

21. Defendant AutoZone is "leading retailer and a leading distributor of automotive replacement parts and accessories in the U.S."[7]

22. Defendant PSC advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[8]

23. Plaintiffs and Class Members are current and former AutoZone employees.

24. As a condition of obtaining employment at AutoZone, Plaintiffs and Class Members were required to entrust Defendants, directly or indirectly, with highly sensitive personal information.

25. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

26. Upon information and belief, Defendants made promises and representations to AutoZone's employees, including Plaintiffs and Class Members, that the PII collected from them as a condition of obtaining employment at AutoZone would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

27. Indeed, AutoZone's Privacy Policy provides that: "[t]he security of your data is important to us . . . we strive to use commercially acceptable means to protect your Personal Information from loss, misuse, and unauthorized access, alteration, disclosure, and destruction[.]"[9]

28. Plaintiffs and Class Members provided their PII, directly or indirectly, to

[7] https://about.autozone.com/
[8] https://www.progress.com/company
[9] https://www.autozone.com/lp/termsAndConditions#privacyPolicy

Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

30. Defendants had duties to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties, and AutoZone had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep consumer's PII safe and confidential.

31. Defendants had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

32. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

34. On or about November 21, 2023, AutoZone, on behalf of Defendants, began

sending Plaintiffs and other Data Breach victims a Notice of Data Incident letter (the "Notice Letter"), informing them that:

> **What Happened?**
>
> AutoZone became aware that an unauthorized third party exploited a vulnerability associated with MOVEit and exfiltrated certain data from an AutoZone system that supports the MOVEit application. As has been widely reported, over two thousand organizations around the world were impacted by the vulnerability in the MOVEit Transfer application. Upon becoming aware of this situation, AutoZone commenced an investigation, retained outside experts, and took measures to assess and remediate incident. We have performed an analysis of the affected system and associated data to determine whether your information was potentially impacted. More specifically, on or about August 15, 2023, AutoZone determined that the exploitation of the vulnerability in the MOVEit application had resulted in the exfiltration of certain data. Based on that analysis, we have determined that certain of your information was included in those files.
>
> **What Information Was Involved?**
>
> Based on our investigation, we understand that your Social Security Number were obtained by an unauthorized third party.[10]

35. Omitted from the Notice Letter were the date that AutoZone became aware of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

36. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. Defendants did not use reasonable security procedures and practices appropriate

[10] Notice Letter.

to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, AutoZone failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

38. The attacker accessed and acquired files from Defendants containing unencrypted PII of Plaintiffs and Class Members, including their Social Security numbers and other sensitive information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

39. The PII of Plaintiffs and Class Members was or will be subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendants Acquire, Collect, and Store Plaintiff's and Class Members' PII

40. As a condition to obtain employment at AutoZone, Plaintiffs and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Defendants.

41. AutoZone retains and stores this information with PSC and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiffs' and Class Members' PII, Defendants would be unable to perform their services.

42. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

43. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members or by AutoZone exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

45. Upon information and belief, AutoZone made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

46. Indeed, AutoZone's Privacy Policy provides that: "[t]he security of your data is important to us . . . we strive to use commercially acceptable means to protect your Personal Information from loss, misuse, and unauthorized access, alteration, disclosure, and destruction[.]"[11]

47. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. *Defendants Knew or Should Have Known of the Risk Because Automotive Service Companies and Software Companies In Possession Of PII Are Particularly Suspectable To Cyber Attacks*

48. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

49. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting automotive service companies

[11] https://www.autozone.com/lp/termsAndConditions#privacyPolicy

and software companies that collect and store PII, like Defendants, preceding the date of the breach.

50. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[12]

51. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

52. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

53. Additionally, as companies became more dependent on computer systems to run their business,[14] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need

[12] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

[13] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

[14] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

for adequate administrative, physical, and technical safeguards.[15]

54. As custodians of PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

56. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

57. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' servers, amounting to more than one hundred thousand individuals' detailed PII,[16] and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

58. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of

---

[15] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

[16] According to the breach report submitted to the Office of the Maine Attorney General, 184,995 persons were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/4b650bee-f556-4b08-8659-f0e1207aa969.shtml

Plaintiffs and Class Members.

59. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

60. In the Notice Letter, AutoZone offers to cover 24 months of credit and identity theft monitoring services for Plaintiffs and Class Members. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

61. AutoZone's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's, or its vendors, computer systems.

62. As an automotive services company and a software company in possession of AutoZone's employees' PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if their data security systems, or those on which it transferred PII, were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value Of PII

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[18]

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[19]

65. For example, PII can be sold at a price ranging from $40 to $200.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

66. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

---

[17] 17 C.F.R. § 248.201 (2013).
[18] *Id.*
[19] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/
[20] *Here's How Much Your PII Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[21] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ .

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

67. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

69. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names and Social Security numbers.

70. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

[22] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

personally identifiable information . . . [is] worth more than 10x on the black market."[23]

71. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

72. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

Defendants Failed to Comply with FTC Guidelines

73. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

74. In October 2016, the FTC updated its publication, Protecting PII: A Guide for

---

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

75. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. These FTC enforcement actions include actions against automotive services companies and software companies, like Defendants.

78. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and AutoZone failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to

protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

79. Defendants were at all times fully aware of their obligations to protect the PII of the employees in their networks yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

80. As noted above, experts studying cybersecurity routinely identify automotive services companies and software companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

81. Some industry best practices that should be implemented by automotive services companies and software companies dealing with sensitive PII, like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

82. Other best cybersecurity practices that are standard in the automotive services and software industries include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

83. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

84. Defendants failed to comply with these accepted standards in the automotive services and software industries, thereby permitting the Data Breach to occur.

Defendants Breached Their Duties to Safeguard Plaintiffs' and the Class's PII

85. In addition to their obligations under federal and state laws, Defendants owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed duties to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of Class Members

86. Defendants breached their obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data, and WelllTok failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect AutoZone's employees' PII;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to sufficiently train their employees and vendors regarding the proper handling of AutoZone's employees' PII;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and,

g. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

87. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access their computer networks and systems which contained unsecured and unencrypted PII.

88. Had Defendants remedied the deficiencies in their information storage and security systems or those of their vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

Common Injuries & Damages

89. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk Of Identity Theft

90. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

91. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

92. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

93. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

94. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

95. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[25]

96. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

97. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it

[25] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than AutoZone credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

98. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

99. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

100. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

101. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

102. Thus, due to the actual and imminent risk of identity theft, AutoZone, in its Notice Letter, instructs Plaintiffs and Class Members to take the following measures to protect themselves:

> We encourage you to review and monitor your account for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information. Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you

should consider taking to protect yourself against fraud and identity theft.[26]

103. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring their own computer networks, contacting financial institutions to ensure their accounts are secured, and monitoring their credit for any indication of fraudulent activity, which may take years to detect.

104. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[27]

105. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[28]

106. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and

[26] Notice Letter.
[27] *See* United States Government Accountability Office, GAO-07-737, PII: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[28] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

time to repair the damage to their good name and credit record."[29]

Diminution Value Of PII

107. PII is a valuable property right.[30] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

108. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[31]

109. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[32,33]

110. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[34]

111. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[35]

---

[29] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[30] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[31] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[32] https://datacoup.com/

[33] https://digi.me/what-is-digime/

[34] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

112. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

113. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names and Social Security numbers.

114. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

115. The fraudulent activity resulting from the Data Breach may not come to light for years.

116. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

117. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to more than one hundred thousand individuals' detailed personal information, upon information and belief, and thus, the

significant number of individuals who would be harmed by the exposure of the unencrypted data.

118. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary

119. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

120. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

121. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

122. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss Of The Benefit Of The Bargain

123. Furthermore, Defendants' poor data security deprived Plaintiffs and Class

Members of the benefit of their bargain. When agreeing to accept employment at AutoZone, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for, or being paid less for, the necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with AutoZone.

PLAINTIFFS' EXPERIENCES

Plaintiff Kevin Walles

124. Plaintiff Kevin Walles is a current AutoZone employee.

125. As a condition of his employment at AutoZone, Plaintiff was required to provide his PII, directly or indirectly, to Defendants, including his name, Social Security number, and other sensitive information.

126. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their systems.

127. Plaintiff Walles is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

128. Plaintiff Walles received the Notice Letter, by U.S. mail, from AutoZone, dated November 21, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

129. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to:

changing passwords and resecuring his own computer networks, contacting financial institutions to ensure his accounts are secured, and monitoring his credit for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time on reasonable efforts to mitigate the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

130. Plaintiff suffered actual injury from having him PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

131. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

132. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

133. As a result of the Data Breach, Plaintiff anticipates spending considerable time

and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

134. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

135. Plaintiff Walles has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jose Vargas

136. Plaintiff Jose Vargas is a former AutoZone employee who worked at AutoZone from approximately 2021 to 2023.

137. As a condition of his employment at AutoZone, Plaintiff was required to provide his PII, directly or indirectly, to Defendants, including his name, Social Security number, and other sensitive information.

138. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their systems.

139. Plaintiff Vargas is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

140. Plaintiff Vargas received the Notice Letter, by U.S. mail, from AutoZone, dated November 21, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his Social Security number.

141. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to:

researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time on reasonable efforts to mitigate the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

142. Plaintiff suffered actual injury from having him PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

143. Plaintiff additionally suffered actual injury in the form of experiencing fraud in the form of an identity thief using his PII to submit a loan application to Upside, in or about November 2023, which, upon information and belief, was caused by the Data Breach.

144. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

146. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff Vargas has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

149. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

150. Specifically, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Class").

151. In addition, Plaintiff Vargas proposes the following California Subclass, subject to amendment as appropriate:

> **California Subclass**
> All individuals in the state of California whose PII was impacted as a result of the Data Breach (the "California Subclass").

152. Excluded from the Classes are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

153. Plaintiffs reserve the right to modify or amend the definition of the proposed

Nationwide Class and/or California Subclass as well as add subclasses, before the Court determines whether certification is appropriate.

154. The proposed Classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

155. Numerosity: The Class Members are so numerous that joinder of all members is impracticable. Although the exact number of Class Members is currently unknown to Plaintiffs and exclusively in the possession of Defendants, according to the breach report submitted to the Office of the Maine Attorney General, at least 184,000 persons were impacted in the Data Breach.[36] The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by AutoZone sending them Notice Letters).

156. Commonality: There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' PII;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII

[36] https://apps.web.maine.gov/online/aeviewer/ME/40/4b650bee-f556-4b08-8659-f0e1207aa969.shtml

compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed duties to Class Members to safeguard their PII;

j. Whether Defendants breached their duty to Class Members to safeguard their PII;

k. Whether hackers obtained Class Members' PII via the Data Breach;

l. Whether Defendants had legal duties to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Defendants breached their duties to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including

injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

157. Typicality: Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

158. Adequacy of Representation: Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

159. Predominance: Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

160. Superiority: A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high

and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

161. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

162. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice Letters by AutoZone.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class against Defendants)

163. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein, and bring this claim against both Defendants.

164. AutoZone requires its employees, including Plaintiffs and Class Members, to submit non-public PII to Defendants in the ordinary course of providing their services.

165. Plaintiffs and the Class Members entrusted their PII to Defendants with the understanding that Defendants would safeguard their information and delete it once the employment relationship terminated.

166. Defendants had full knowledge of the sensitivity of the PII and the types of harm

that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

167. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants owed duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. AutoZone's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

168. Defendants had duties to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

169. Defendants owed duties of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

170. Defendants' duties of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of being employees at AutoZone.

171. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

172. Defendants were subject to an "independent duty," untethered to any contract

between Defendants and Plaintiffs or the Class.

173. Defendants also had duties to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

174. Moreover, Defendants had duties to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

175. Defendants had and continues to have duties to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

176. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former employees' PII it was no longer required to retain

pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

177. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

178. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

179. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

180. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

181. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

182. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was

reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the automotive services and software industries.

183. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

184. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

185. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

186. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

187. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

188. Defendants' duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

189. AutoZone has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

190. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

191. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

192. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Vargas experiencing fraud in the form of an identity thief using his PII to submit a loan application to Upside, in or about November 2023; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

193. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic

losses.

194. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

195. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

196. Defendants' negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

197. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class against Defendant AutoZone)

198. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein and brings this count solely against Defendant AutoZone ("Defendant" for the purposes of this count).

199. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their employment at AutoZone.

200. Plaintiffs and the Class entrusted their PII to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard

and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

201. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

202. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

203. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

204. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

205. In accepting the PII of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

206. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the

Data Breach.

207. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

208. Plaintiffs and Class Members provided their labor and PII to AutoZone with the reasonable belief and expectation that Defendant would use part of their earnings to obtain adequate data security. Defendant failed to do so.

209. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

210. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

211. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

212. Defendant breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

213. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

214. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

215. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class against Defendants)

216. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein, and bring this claim against both Defendants.

217. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they provided their labor to AutoZone and in so doing also provided Defendants with their PII. In exchange, Plaintiffs and Class Members should have received from AutoZone the employment position that was the subject of the transaction and should have had their PII protected with adequate data security.

218. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

219. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

220. Defendants acquired the PII through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

221. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and

secure their PII, they would have entrusted their PII at Defendants or obtained employment at AutoZone.

222. Plaintiffs and Class Members have no adequate remedy at law.

223. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

224. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Vargas experiencing fraud in the form of an identity thief using his PII to submit a loan application to Upside, in or about November 2023; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

225. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

226. Plaintiffs and Class Members may not have an adequate remedy at law against

Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violation of the California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)
(On Behalf of Plaintiff Vargas and the California Subclass against Defendant AutoZone)

227. Plaintiff Vargas ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count) solely against Defendant AutoZone ("Defendant" for the purposes of this count).

228. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> >
> > (B) Injunctive or declaratory relief.
> >
> > (C) Any other relief the court deems proper.

229. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of their shareholders or other owners, with gross revenues in excess of $25 million.

230. Plaintiff and Class Members are covered "consumers" under § 1798.140(g) in that

they are natural persons who are California residents.

231. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

232. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violations of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

233. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and Class Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

234. As a direct and proximate result of Defendant's acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

235. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

236. On November 29, 2023, Plaintiff provided AutoZone with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant fails to respond, have not cured, or are unable to cure the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

237. Accordingly, Plaintiff and the Class Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

COUNT V
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
Cal Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff Vargas and the California Subclass against Defendant AutoZone)

238. Plaintiff Vargas ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count) solely against Defendant AutoZone ("Defendant" for the purposes of this count).

239. By reason of the conduct alleged herein, Defendant engaged in unfair and unlawful "business practices" within the meaning the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

240. Defendant stored the PII of Plaintiff and the Class Members in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and the Class Members' PII a secure and prevented the loss or misuse of that PII.

241. Plaintiff and Class Members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PII safe.

242. Defendant did not disclose at any time that Plaintiff's PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose.

243. Defendant violated the UCL by failing to maintain the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

244. Defendant violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, failing to audit, verify, and monitor the data security practices of its

vendors, and by failing to immediately timely and adequately notify Plaintiff and Class Members of the Data Breach.

245. Section 5 of the FTCA required Defendant to take reasonable measures to protect Plaintiff's and the Class Member's PII data and is a further source of Defendant's duty to Plaintiff and the Class Members.

246. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to implement and use reasonable measures to protect Sensitive Information. Defendant, therefore, was required and obligated to take reasonable measures to protect PII it solicited, possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duty to adequately protect Sensitive Information. By failing to implement and use reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

247. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from, Defendant's failure to timely notify Plaintiff and the Class Members of the Data Breach.

248. Moreover, Defendant's collection of sensitive employees' PII in combination with its failure to implement reasonable security safeguards demonstrate Defendant's violation of the unfair prong of the UCL.

249. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment. These unfair

acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

250. Plaintiff and Class Members have lost money and property as a result of Defendant's violations of the UCL as they were denied the benefit of their transacting with Defendant because Defendant failed to use funds to supply adequate data security.

251. Moreover, Plaintiff and Class Members provided their PII to Defendant, which is property as defined by the UCL, and their property has been diminished in value as a result of the loss of its confidentiality.

252. Plaintiff and Class Members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Vargas experiencing fraud in the form of an identity thief using his PII to submit a loan application to Upside, in or about November 2023; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

253. Unless restrained and enjoined, Defendant will continue to engage in the above-

described wrongful conduct and more data breaches will occur.

254. As such, Plaintiff, on behalf of himself and Class Members, seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

255. To the extent any of these remedies are equitable, Plaintiff and the Class seek such equitable remedies, in the alternative to any adequate remedy at law they may have.

COUNT VI
Invasion of Privacy
Cal. Const. Art. 1 § 1
(On Behalf of Plaintiff Vargas and the California Subclass against Defendant AutoZone)

256. Plaintiff Vargas ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the "Class" for the purposes of this count) solely against Defendant AutoZone ("Defendant" for the purposes of this count).

257. California established the right to privacy in Article I, Section 1 of the California Constitution.

258. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

259. Defendant owed a duty to its current and former employees, including Plaintiff and the Class, to keep their PII contained as a part thereof, confidential.

260. Defendant failed to protect and released to unknown and unauthorized third

parties the PII and of Plaintiff and the Class.

261. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class, by way of Defendant's failure to protect the PII.

262. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class is highly offensive to a reasonable person.

263. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII to Defendant as part of obtaining employment at AutoZone, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

264. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

265. Defendant acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

266. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

267. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

268. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII and maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come.

269. Plaintiff, on behalf of the Class, seeks injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

270. Plaintiff's and Class Members' PII, which remains in Defendant's possession, will be subject to further disclosure unless and until this Court compels Defendant to audit and strengthen the security of its data systems.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and California Subclass, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering

Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed

in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 29, 2023

Respectfully submitted,

/s/ Randi Kassan

Randi Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

Counsel for Plaintiffs and the Proposed Class